

**UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA**

---

United States of America,

Case No. 20-cv-233 (JRT/DTS)

Plaintiff,

v.

**REPORT AND RECOMMENDATION**

Abdou Diallo (9),

Defendant.

---

**INTRODUCTION**

Defendant Abdou Diallo moves to suppress evidence obtained through search of his email account, arguing the underlying warrant was invalid because (1) the application failed to establish a nexus with criminal conduct; (2) the application was based on stale information; and (3) the warrant was overbroad. Diallo further contends the good faith exception does not apply and all evidence obtained from the search of his email should be suppressed. Because the email search warrant was supported by probable cause and the good faith exception applies in any event, the Court recommends Diallo's Motion to Suppress Evidence Obtained as a Result of Search and Seizure [Dkt. No. 233] be denied.

**FINDINGS OF FACT**

**I. The Broader Fraudulent Scheme**

In September 2019, federal investigators applied for a warrant to search seven email accounts, including that belonging to the Defendant. Response to Mot. by USA, Ex. B (Warrant); Dkt. No. 257-1. Postal Inspector John Western's affidavit in support of the warrant application detailed a wide-ranging and years-long scheme, stretching back to at least 2011, involving fraudulent magazine telemarketing. Numerous companies

purporting to be magazine subscription services used a similar roadmap to defraud customers. *Id.*, 1-21.

For example Your Magazine Service, one of the fraudulent companies, carried out the following scheme: First, its employees used a call script when talking to customers. The scripts introduced the caller as the customer's magazine service. They next stated that because the customer had made on-time payments the caller was authorized to reduce the customer's outstanding balance by crediting the customers' credit card. *Id.* at 6. Oftentimes, the caller would get a "closer" on the line, who would state they were the caller's supervisor and was making sure the caller had provided good service. *Id.* at 7. The closer would then trick the customer into providing their credit card information before sowing further confusion by offering to reduce the overall number of payments left on their account, but actually signing the customer up for additional subscriptions. *Id.*

To illustrate further: the caller would falsely state the customer currently owed \$49.90 per month, and that the caller could reduce the overall number of monthly payments by three months, saving the customer \$150. *Id.* But the customer did not actually owe any monthly payments, and instead the fraudster was creating new charges for \$49.90 per month. *Id.* If a customer resisted these offers, the company would reassure them the customer was not signing up to receive *more* magazines and was simply getting a discount. *Id.* at 8-9. The fraudsters would record the end of the call, where they purported to "confirm" this arrangement with the customer. *Id.* at 9.

Other companies' playbook was nearly identical. See *id.* at 17-21. Sometimes companies offered to stop billing customers so long as the customer made large lump sum payments on their magazine accounts, only for their normal monthly payments to

continue. *Id.* at 16. Those customers had monthly magazine subscriptions, but the fraudsters were not the servicers and were not reducing the overall payments the customer owed. *Id.*

In 2018, the government indicted the owner of Your Magazine Service, Individual A, and continued investigating the network of companies possibly involved in this conduct. *Id.* at 11. In the hopes of receiving a reduced sentence for his crimes, Individual A provided information and other assistance to the US Attorney's Office investigation. *Id.* at n.2. According to Individual A, there were at least 10-15 other fraudulent magazine companies in Minnesota, with many more spread across the country. *Id.* Victims of this scheme often had multiple charges every month from various magazine companies, totaling hundreds of dollars monthly. *Id.* at 13-16.

Individual A explained that the scheme relied on "lead lists"—lists of potential customers the fraudsters could call to try to make a "sale." *Id.* at 12. Lead lists contained customer names, phone numbers, and other contact information. Some also included whether the customer had active, legitimate magazine subscriptions and payment method for that subscription. *Id.* Lead lists with the best potential customers "could sell for up to several dollars per name." *Id.* The network of fraudulent magazine companies would share and exchange lead lists. *Id.* In particular, these companies used "Paid-during-service" (PDS) lists to perpetrate their fraud. *Id.* at 21. PDS lists are lists of people who have existing magazine subscription. *Id.*

Over his years of defrauding customers, Individual A communicated with Brian Cox who sold Individual A lead lists many times. *Id.* Their communications dated to at least 2012. *Id.* at 21. In July 2019, Cox contacted Individual A, who agreed to record a phone

call between himself and Cox, where he offered Cox lead lists. *Id.* at 22. He told Cox the lists were “premium shit,” “spendy but not hammered stuff . . . [The customers] haven’t been handed around. They haven’t been beaten up. They haven’t been crucified.” *Id.* at 23. Cox explained he had “six guys that religiously buy leads from me every week” and agreed to distribute the lists and split profits from their sale with Individual A. *Id.* at 23. Cox followed through, emailing several people on July 16, 2019, offering lead lists for 7 items, including “HOTPDS-Premium Hand Writes!!! \$5 each. I’ve got 50 records in hand. 2000 of this same exact Hand Writes Available.” *Id.* at 23; Def. Ex. 6; Dkt. No. 236-6. In reality, the lists Individual A sent Cox were fake and listed Postal Inspectors operating undercover to learn about the fraud. *Id.* at 24. Shortly after distributing the list, undercover Postal Inspectors began receiving calls from magazine companies, who called using scripts similar to those described above. *Id.* Investigators then searched Cox’s email pursuant to a warrant. *Id.*

## **II. Diallo’s Communications with Cox**

One of the recipients of Cox’s July 16, 2019 email was the defendant, Abdou Diallo. Diallo replied a few minutes after receiving the message, requesting “please send the sample [of ‘HOTPDS-Premium Hand Writes’] so we can see the quality of it so let us try the 50 names.” Def. Ex. 12; Dkt. No. 236-12. Search of Cox’s email account uncovered other communications with Diallo dating back to 2015 including:

1. Cox sent Diallo 93 handwritten records (leads), containing customer name, address, date of last sale, salesperson, closer and verifier, type of credit card, last four digits of the credit card number, and credit card expiration date. *Id.* at 34.

2. Cox offered PDS lists. He stated his source was “pulling in \$20K per week.” *Id.* at 34-35.
3. Cox and Diallo communicated about sales scripts. First, Cox sent a script, with Diallo replying with a similar but not identical script and remarking that the other one caused “to many chargebacks.” Diallo described his script as “clean.” *Id.* at 35-36; Def. Ex. 3; Dkt. No. 236-3.
4. Cox offered lead lists in 2018. Warrant at 36; Dkt. No. 257-1.
5. Cox emailed Diallo with two invoices covering “200 records,” to which Diallo replied, “Thank you will send payment now.” *Id.* at 36; Def. Ex. 4; Dkt. No. 236-4.

The warrant at issue also detailed a whistleblower formerly employed by other recipients of Cox’s July 16, 2019, email who described her former employer as “a scam,” and described the employer’s use of the same process Individual A used to defraud customers. *Id.* at 25. In addition, the Better Business Bureau had received complaints about multiple companies implicated by Cox’s email. *Id.* at 25, 38-39.

Magistrate Judge Tony Leung issued the warrant. *Id.* at 1. Diallo now moves to suppress all evidence obtained through the resulting search.

## **CONCLUSIONS OF LAW**

### **I. Nexus with Criminal Conduct**

The Fourth Amendment prohibits “unreasonable searches and seizures,” and provides that law enforcement may only obtain a warrant “upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const., amend. IV. “Whether probable cause

to issue a search warrant has been established is determined by considering the totality of the circumstances.” *United States v. Notman*, 831 F.3d 1084, 1088 (8th Cir. 2016). To be valid, a warrant must set forth “sufficient facts to lead a prudent person to believe that there is a fair probability that contraband or evidence of a crime will be found in a particular place” *Id.* The totality-of-the-circumstances test for reviewing a probable cause determination means that such inquiries are “not readily, or even usefully, reduced to a neat set of legal rules.” *Florida v. Harris*, 568 U.S. 237, 243 (2013). While judges issuing search warrants may “draw reasonable inferences from the totality of the circumstances” *United States v. Keele*, 589 F.3d 940, 944 (8th Cir. 2009) (quoting *United States v. Alexander*, 574 F.3d 484, 490 (8th Cir. 2009)), a warrant issued based only on a supporting affidavit that merely asserts conclusions rather than facts may be invalid. *Aguilar v. Texas*, 378 U.S. 108, 113 (1964) (internal citations omitted).

Reviewing courts must afford “great deference” to the probable cause determination of the judge who issued the warrant and should resolve even “doubtful or marginal cases” in favor of a warrant’s validity. *United States v. Butler*, 594 F.3d 955, 962 (8th Cir. 2010) (citation omitted); see *United States v. Ventresca*, 380 U.S. 102, 109 (1965). So long as the issuing judge had a “substantial basis” for concluding the “search would uncover evidence of wrongdoing,” this Court must uphold the probable cause determination. *United States v. Horn*, 187 F.3d 781, 785 (8th Cir. 1999).

Diallo first argues the warrant was invalid for lack of a nexus with criminal activity. In short, he contends the warrant application fails the Fourth Amendment’s requirement that there be a “fair probability that contraband or evidence of crime will be found in a particular place.” Def. Mem. of Law in Support of Mots. To Suppress Evidence From

Search and Seizure (Def. Mem.) at 5; Dkt. No. 236 (citing *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). Diallo notes that he was but one recipient of emails Cox sent to several people. Def. Mem. at 5; Dkt. No. 236. He also points out that it was Cox rather than Diallo himself who initiated contact. *Id.* at 6. He alleges that the receipt of a sales script or lead lists is not necessarily evidence of a crime, scripts and lead lists being common tools used by legitimate telemarketers. *Id.* at 5. In particular, Diallo points out that his correspondence about scripts involved scripts he characterized as “clean.” *Id.* Diallo describes all of this as “innocuous.” *Id.* at 6.

Looking at these interactions individually, it certainly appears possible that Diallo’s conduct was innocuous. But looking at them within the totality of the circumstances detailed in the warrant affidavit, this conduct could just as easily indicate criminal activity. The warrant application explained the scheme Diallo was suspected of engaging in, including its use of lead lists and scripts; it suggested Cox believed Diallo would buy the lead lists full of names of people who hadn’t been “crucified”. *Id.* at 22-23. Lists Diallo purchased contained the same types of information Individual A described, as well as references to “closers.” *Id.* at 34. While Diallo described the script he sent Cox as “clean” that does not necessarily indicate Diallo was not involved in the fraud; it could just as easily demonstrate he had been using a “dirty” script and now was trying out a different approach.

Moreover, the affidavit established that others who bought those fake lead lists employed the lists, calling the undercover Postal Inspectors and reciting scripts as described in the affidavit. Diallo argues that his “mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to

search that person,” *Id.* at 4 (quoting *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979)). But the link between Diallo’s conduct and the others named in the search warrant was more than the “mere propinquity” seen in *Ybarra*. In *Ybarra*, a warrant authorized police officers to search a bar and its bartender for evidence of drug possession. *Id.* at 88. After entering the bar, the officers told every person present that they were going to search for weapons and then patted down nine of the thirteen bar patrons including Ybarra. *Id.* After feeling “a cigarette pack with objects in it” during Ybarra’s patdown, officers fully searched him and recovered tinfoil packets containing heroin. *Id.* at 89. The Supreme Court suppressed that evidence, explaining that

There is no reason to suppose that, when the search warrant was issued . . . the authorities had probable cause to believe that any person found on the premises of the [bar], aside from the [bartender] would be violating the law. The search warrant complaint did not allege that the bar was frequented by persons illegally purchasing drugs. It did not state that the informant had ever seen a patron of the tavern purchase drugs from [the bartender] or from any other person. Nowhere, in fact, did the complaint even mention the patrons of [the bar].”

*Id.* at 90.

Diallo was not merely at a bar where a suspected criminal happened to work. Diallo was conversing via email with Cox, from whom Individual A had obtained lead lists for use in the scheme. Diallo was included on emails with others who had contacted undercover Postal Inspectors using the same lists Diallo had purchased. Diallo himself had paid Cox for lead lists in the past and conversed with him about phone scripts. All things considered, this conduct could be criminal. See *Harris*, 568 U.S. at 243 (noting the “totality of the circumstances” test for probable cause). The Court reiterates that Diallo could be correct that his conduct cited in the warrant affidavit was innocuous. He is innocent until proven guilty. Nevertheless, the warrant application established a nexus



between Diallo and suspected criminal activity and his argument to the contrary accordingly fails.

## **II. Staleness**

Diallo also objects to the warrant contending it was based on stale information. There is “no fixed formula” for determining when information becomes stale. *United States v. Petruk*, 929 F.3d 952, 960 (8th Cir. 2019) (quoting *United States v. Nieman*, 520 F.3d 834, 839 (8th Cir. 2008); see also *United States v. Koelling*, 992 F.2d 817, 822 (8th Cir. 1993) (“There is no bright-line test for determining when information is stale.”). Instead, courts assess the property subject to search and the nature of the alleged criminal act. *Id.* Where a crime is “of a continuous nature” the passage of time between obtaining the information and executing the search is “less significant.” *Id.* (quoting *United States v. Maxim*, 55 F.3d 394, 397 (8th Cir. 1995)).

Diallo argues the emails between Cox and Diallo began in 2015 and carried on through 2019. Yet, he notes, some of those communications were one-way; Cox’s messages went unanswered. Further, there was a “several year void” in the communications and Diallo’s subsequent contact with Cox was “innocuous.” Def. Mem. at 8; Dkt. No. 236; see also Supplemental Memorandum of Law in Support of Mot. to Suppress Evidence from Search and Seizure (Def. Supp. Mem.) at 6-7; Dkt. No. 262. He argues that only one email sent in 2015 “suggests possible misconduct” and that email “should not be conflated with” later emails. Thus, there was no “continuous” conduct and the four-year gap between the 2015 email and the 2019 search warrant renders the warrant’s supporting information stale.

Diallo asks the Court to read the warrant application too narrowly. As Diallo correctly points out, staleness “depends on the circumstances of the case, including the nature of the crime under investigation.” Def. Mem. at 7; Dkt. No. 236 (citing *Koelling*, 992 F.2d at 822). Here, the warrant application averred that Individual A had been defrauding people with this scheme since at least 2011, that Cox’s lead lists had helped Individual A perpetrate his fraud, and the Cox believed Diallo would be interested in lead lists. Warrant at 13, 21-23, 34; Dkt. No. 257-1. It also established that Diallo had been in contact with Cox periodically about lead lists. *Id.* at 34-37. Again, that those communications may have been innocent does not preclude the possibility that they were illicit. Taken together and “examin[ing staleness] in the context of a specific case and the nature of the crime under investigation” the four-year-old information in the warrant was not stale as a matter of law. *Koelling*, 992 F.2d at 822.

### **III. Overbreadth**

Federal Rule of Criminal Procedure 41(e)(2)(B) provides a two-step process for search and seizure of electronic storage media. Under that rule “[a] warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified the warrant authorizes a later review of the media or information consistent with the warrant.” The framers of that rule explained that under the two-step process “officers may seize or copy *the entire storage medium* and review it later to determine what electronically stored information falls within the scope of the warrant.” *United States v. Beckmann*, 786 F.2d 672, 680, n.6 (8th Cir. 2015) (quoting Fed. R. Crim. P. 41, Advisory Committee’s Note on 2009 Amendments (emphasis added)).

The warrant at issue here was a two-step warrant. At Step One, the application detailed the “particular things to be seized,” which included “[t]he contents of all e-mails associated with the account.” Warrant at 48. Step Two detailed the “information to be seized by the government” which narrowed those things listed in Step One. Step Two sought “All information described above [] that constitutes fruits, contraband, evidence and instrumentalities of violations of [18 U.S.C. § 1343]” involving certain people and companies, “occurring on or after 2011.” *Id.* at 49. Diallo contends each step of this warrant was overbroad, failing the Fourth Amendment’s particularity requirement. Def. Mem. at 10; Dkt. No. 236; see *also* Supp. Def. Mem. at 7-8; Dkt. No. 262. To be sufficiently particular, the warrant application must describe the items to be seized with enough detail that “the searcher [can] locate and identify the places and items with reasonable effort and [] avoid mistakenly searching the wrong places or seizing the wrong items.” *United States v. Gleich*, 397 F.3d 608, 911 (8th Cir. 2005). Courts evaluate particularity for “practical” not “hypertechnical” accuracy. *United States v. Fiorito*, 640 F.3d 338, 346 (8th Cir. 2011). As with staleness, particularity depends in part on the nature of the investigated crimes. See *United States v. Frederickson*, 846 F.2d 517, 519 (8th Cir. 1988); *United States v. Cooper*, 654 F.3d 1104, 1127 (10th Cir. 2011); *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001). This approach comports with the totality-of-the-circumstances test for probable cause in general. See *Notman*, 831 F.3d at 1088.

Diallo argues that Step One of the warrant was overbroad for lack of procedural safeguards. Def. Mem. at 10; Dkt. No. 236. Because according to Diallo the Government could have required key word searches prior to seizure of the account, or segregated investigators conducting the search thereby cutting down on how many emails were

turned over, the warrant was overbroad. *Id.* But those types of key word searches and taint team processes are precisely what is contemplated by Step Two of the warrant application. Here, at Step Two the Government provided detailed representative lists of items to be seized, limiting seizure to only those documents, records, and communications that related to specific companies, “other magazine sales companies, communications with magazine companies, magazine telemarketers, publishers, magazine brokers, lead list brokers, employees, telemarketing brokers, software companies, debt collectors, debt collections companies, magazine fulfillment representatives and companies, credit card processing representatives and companies and magazine customers.” Warrant at 49; Dkt. No. 257-1.

The Eighth Circuit and courts within its jurisdiction have repeatedly found broad lists of documents sufficiently particular to support a warrant. For example, in *Fiorito*, law enforcement obtained a warrant to search the defendant’s “residence for incriminating documents” including “entire files involving Fiorito.” *United States v. Fiorito*, 640 F.3d 338, 346-47. Fiorito objected, arguing the warrant application was not sufficiently particular. But the Eighth Circuit disagreed, noting the “extensive list of specific documents sought” that followed the broad introductory language Fiorito cited. *Id.* at 347. The Court further instructed that the practical rather than hypertechnical assessment of particularity supports the search as well, because “[t]he warrant did not authorize a blanket search of documents for no particular purpose, but rather for the purpose of discovering evidence of an ongoing, well-defined, equity-stripping scheme.” *Id.*, see also *United States v. Adams*, 17-cr-64, 2018 WL 6991106, at 31 (D. Minn. Sept. 17, 2018).

The same principles apply in this case as well. Here, the first step of the warrant application acts as “broad introductory language,” teeing up Step Two, which includes an “extensive list of specific documents sought.” *Fiorito*, 640 F.3d at 347. In *Fiorito*, authorities were authorized to search the entirety of Fiorito’s house, but they were only looking for “specific documents.” Here, the warrant application asked for authorization to search the entirety of Diallo’s email (Step One), but *only* for those items listed in Step Two. As a practical matter, this is the only way such a search could work. A taint team can only filter out unauthorized documents, content, or items if they first have the larger body of documents, content, or items from which to filter. Nor is asking the email providers to do taint team-like searches in advance of the Government a solution. It is both impractical and also legally dubious to ask a private entity to sift through another’s information at the behest of the Government. There is no basis to conclude that a private email service provider would choose to open itself up to scrutiny for such conduct.

Next, just as the warrant in *Fiorito* made plain the purpose of the search, so too did the warrant here. The warrant application included over forty pages of information describing the background of the alleged fraud, the tools used to commit the fraud, the various actors believed to be involved, etc. The attachment detailing the two steps of this warrant specifically cited a section of the U.S. Code at issue and specific types of information sought which clearly related to crimes under that code section and the conduct described in the warrant affidavit. This was not a “blanket” application with no purpose. See *Fiorito*, 640 F.3d at 347; *Adams*, 2018 WL 6991106 at \*31.

Diallo also contends the warrant was overbroad at Step Two specifically, because it sought emails dating back to 2011, yet the warrant application only included information

about Diallo dating back to 2015. *Id.* As explained above, the warrant application established that the broader scheme had been going on since at least 2011. While Cox's emails with Diallo only date to 2015, those emails suggested that Diallo was already involved in magazine telemarketing at the time of those emails. Cox was not introducing Diallo to lead lists and scripts for the first time; instead they were conferring about purchasing lead lists and using scripts in what appeared to be a continuing practice. Warrant at 34-37; Dkt. No. 257-1. Because the totality of the warrant application suggests this scheme had been ongoing since at least 2011 and particularity depends on the nature of the specific investigated crimes, the warrant was not overbroad based on its time period. *See Frederickson*, 846 F.2d at 519.

The Court is aware of the decision in *United States v. Moulder*, 20-cr-232, 2022 WL 3644893 (D. Minn. August 24, 2022). If the District Court determines that decision mandates a different finding as to particularity, this Court still recommends Diallo's motion be denied because the good faith exception would apply, as detailed below.

#### **IV. Good Faith Exception**

Even if the warrant lacked probable cause to be issued, the good faith exception would apply here, precluding suppression of evidence borne from the search. Under the good faith exception to the Fourth Amendment's warrant requirement, "disputed evidence will be admitted if it was objectively reasonable for the officer executing the search warrant to have relied in good faith on the judge's determination that there was probable cause to issue the warrant." *United States v. Mayweather*, 993 F.3d 1035, 1041 (8th Cir. 2021). "The operative test is whether a reasonably well trained officer would have known that the search was illegal despite the issuing judge's authorization." *Id.* (internal quotation

marks and citations omitted). There are four recognized limits to the good faith exception.

The exception will not apply

(1) when the affidavit or testimony supporting the warrant contained a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge; (2) when the issuing judge wholly abandoned his judicial role in issuing the warrant; (3) when the affidavit in support of the warrant is so lacking in indicia of probable cause as to render official belief in its existence *entirely unreasonable*; and (4) when the warrant is so facially deficient that no police officer could reasonably presume the warrant to be valid.

*United States v. Proell*, 485 F.3d 427, 431 (8th Cir. 2007) (citing *United States v. Leon*, 468 U.S. 897, 921 (1984)). As with warrant analysis is general, courts consider the totality of the circumstances in determining whether a law enforcement officer's reliance on the warrant was done in good faith. *United States v. Grant*, 490 F.3d 627, 632 (8th Cir. 2007).

Diallo contends the first limit is implicated, not because the affiant provided "deliberately falsified information" but rather because the affiant "report[ed] less than the total story." *Id.* at 12; citing *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir. 1985). But while Diallo need not provide "clear proof" of a false statement within the warrant application, he is required to make a "substantial showing that the affiant intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading." *Stanert*, 762 F.2d at 781.

Diallo has not made such a showing here. While Diallo contends the affidavit grouped information in a way that misled the magistrate, and that the affidavit included unfair leaps in logic, Def. Mem. at 14-15, those contentions do not rise to the "significant showing" required to preclude suppression. This argument again amounts to a claim that Diallo's conduct was innocuous, not illegal. While Diallo may very well be innocent and

his conduct legitimate, that possibility does not establish that the affiant misled the magistrate. Absent such a showing, the good faith exception applies here.

Diallo also argues that all the alleged deficiencies with the warrant application detailed above implicate the third limit to the good faith exception: the affidavit was so lacking in indicia of probable cause that reliance on its existence was unreasonable. Def. Mem. at 13; Dkt. No. 236. Diallo notes that the same law enforcement officer applied for and executed the warrant, suggesting his reliance on it was not in good faith because he knew from having falsified the application that the warrant was invalid. But this argument assumes bad faith by the officer in order to demonstrate that the officer acted in bad faith. The warrant application set forth details of the alleged telemarketing fraud, including details about the use of lead lists and call scripts; it established that Brian Cox had provided lead lists to Individual A, and that Cox had what appeared to be an ongoing, if sporadic, correspondence with Diallo. For the reasons cited above, any problem with staleness, overbreadth, or criminal nexus is not so obvious that an officer could not rely on the warrant in good faith.

Lastly, to the extent the decision in *Moulder*, 2022 WL 3644893, gives an officer reason to question the validity of a two-step warrant such that the good faith exception would not apply, that argument is moot in this case. Here, the warrant long predated the decision in *Moulder*, the warrant having issued in September 2019 and the *Moulder* decision having issued in August 2022.

## **V. Fruit of the Poisonous Tree**

Lastly, law enforcement executed a second search of Diallo's email pursuant to a different search warrant. Diallo contends that search was the fruit of the poisonous tree



of the first search. For the reasons explained above, the first email warrant was valid and, even if it were not, the good faith exception would apply. Diallo's argument thus fails.

### **RECOMMENDATION**

For the reasons set forth above, the Court RECOMMENDS THAT: Diallo's Motion to Suppress Evidence Obtained as a result of Search and Seizure [Dkt. No. 233] be **DENIED.**

Dated: April 5, 2023

\_\_\_\_\_  
s/David T. Schultz  
DAVID T. SCHULTZ  
United States Magistrate Judge

### **NOTICE**

**Filing Objections:** This Report and Recommendation is not an order or judgment of the District Court and is therefore not appealable directly to the Eighth Circuit Court of Appeals.

Under Local Rule 72.2(b)(1), "a party may file and serve specific written objections to a magistrate judge's proposed finding and recommendations within 14 days after being served a copy" of the Report and Recommendation. A party may respond to those objections within 14 days after being served a copy of the objections. LR 72.2(b)(2). All objections and responses must comply with the word or line limits set for in LR 72.2(c).